ITC RECOMMENDED POLICIES & GUIDELINES

VIRUS PROTECTION POLICY & PROCEDURES

Section 1. Purpose and Scope.

1.1. Purpose.

1.1.1. To protect WVBEP computers and data networks against virus infections to an extent consistent with cost-effectiveness and without interfering unnecessarily with the productive use of its computers and networks.

1.1.2. To establish a policy and procedure that defines the responsibilities for reducing the threat of computer viruses to WVBEP computers and networks.

1.1.3. To establish responsibility for overseeing computer virus prevention activities within the WVBEP and to establish a reporting mechanism to ensure that all appropriate personnel are contacted in case of a computer virus incident.

1.1.4. To promote WVBEP employee awareness of the threat posed by computer viruses and to ensure that virus protection software and procedures are properly implemented and utilized on a regular basis.

1.2. Scope.

1.2.1. Compliance with the provisions of the policy concerning pre-scanning of all data and program files before installation and reporting of possible viruses applies to anyone performing work using computer resources within the WVBEP.

1.2.2. Violations of this policy will subject an individual to disciplinary action ranging from a warning, suspension of privileges, or dismissal from the WVBEP and prosecution under state and/or federal statutes - depending on the circumstances of the incident.

Section 2. Definition of Terms.

2.1. Authorized Software: See the WVBEP Computer Software Policy.

2.2. Computer Virus: A computer virus is a program or piece of code that is loaded onto any computer, including PCs and servers, without the knowledge of the owner and runs against the owner's wishes. All computer viruses are manmade. All computer viruses will disrupt the operation of the infected computer. Some computer viruses are destructive, permanently damaging data files or programs on a computer.

2.3. Virus Coordinator: A Virus Coordinator is an individual designated by a Division Director to coordinate virus protection activities at a remote office location. A remote office is any WVBEP office located outside of Charleston and/or where the WVBEP MIS Division does not have support staff nearby to respond rapidly to a virus 'attack'.

Section 3. Policy Notification.

3.1. Any individual requiring the use of a WVBEP computer and/or network shall be made aware of this policy by the supervisor granting access to the WVBEP computer and/or network prior to being granted access. The individual must indicate in writing that s/he has read this policy by signing in the space provided on the last page of this policy.

Section 4. Responsibilities.

4.1. Each Individual WVBEP Division's Responsibility.

4.1.1. It is each Division's responsibility to identify and make available one or more standalone PCs for use in scanning incoming data and program files for potential viruses. The minimum specifications for these PCs shall be maintained by the WVBEP MIS Division on the WVBEP Intranet page.

4.1.2. Division Directors shall designate a Virus Coordinator at each remote office location of their Division to assume the responsibility for coordinating virus protection activities for the office location with the WVBEP MIS Division. The Division Directors will notify all Division staff, as well as the Directors of all other WVBEP Divisions, who has been designated as the Virus Coordinator(s).

4.2. Every Employee's Responsibility.

4.2.1. Each employee is personally responsible for understanding and observing the provisions of this policy.

4.2.2. It is contrary to WVBEP policy for any employee to introduce, deliberately, a virus into WVBEP computers and/or networks, to withhold information necessary for the effective implementation of virus protection procedures or to use software or data that has not been properly scanned for viruses in WVBEP computers and/or networks.

4.3. WVBEP MIS Division's Responsibility.

4.3.1. The WVBEP MIS Division is responsible for overseeing computer virus protection activities within the WVBEP.

4.3.2 The WVBEP MIS Division will evaluate, recommend, and maintain virus protection software and/or tools for use on WVBEP desktop computers and network servers. The WVBEP MIS Division will provide support for the evaluation, acquisition, and maintenance of virus protection software and/or tools for other systems maintained within the WVBEP. The WVBEP MIS Division will ensure that virus protection software is installed on any desktop computer and network server acquired by WVBEP before they are made available for use by WVBEP, its employees or its agents.

4.3.3. The WVBEP MIS Division will coordinate any training on virus control required for Virus Coordinators and WVBEP personnel in general. [This training will include the development and distribution of posters warning all WVBEP personnel of the dangers of computer viruses.]

4.3.4. The WVBEP MIS Division will investigate every report of an apparent computer virus infection, and will make every reasonable effort to determine the source of the infection. The WVBEP MIS Division will keep all affected personnel advised of the investigation.

4.3.5. For each incident, The WVBEP MIS Division will develop and/or provide step-by-step procedures for the scanning and actual removal of the virus.

4.3.6. The WVBEP MIS Division will oversee the effort to remove the virus from the affected computer, to scan for viruses on any other computers that were connected to this computer, and to scan any diskettes that were used in the computer(s).

Section 5. Virus Protection Procedures.

5.1. General Guidance

5.1.1. All data and/or program files must be scanned for viruses before installation (or, in the case of software distributed in compressed form, immediately after installation) to safeguard WVBEP networks from infection. This includes shrink-wrapped software (i.e., software shipped in tamper-proof packaging) procured directly from commercial sources such as Microsoft, Novell, etc. It also includes shareware and freeware obtained from electronic bulletin boards or on disk (diskette or CD-ROM), custom-developed software, and software received through business sources (such as DoL, other state agencies, federal agencies, regulated companies, consultants, law offices, etc.).

5.1.2. All data and program files that have been electronically transmitted to a WVBEP computer from another location, internal or external, must be scanned for viruses immediately after being received.

5.1.3. Every diskette is a potential source for a computer virus. Therefore, every diskette must be scanned for virus infection before it is used in a WVBEP computer or network server.

5.1.4. Computers and/or network servers shall never be "booted" from a diskette received from an outside source. Users shall always remove a diskette from the disk drive when not in use. This is to ensure that the diskette is not in the disk drive when the machine is powered on. A diskette infected with a boot virus may infect a computer in that manner, even if the diskette is not a "bootable" diskette.

5.1.5. Virus protection software shall be loaded on each desktop computer and server as a terminate and stay resident (TSR) program to constantly monitor for viruses to prevent introduction to the network.

5.1.6. Whenever possible, one PC in each office location should have a "scan disk" with the scanning software files on it or a PC with the scanning software loaded on the hard disk drive. This 'scanning' PC should be independent from any WVBEP network.

5.2. Virus Reporting and Documentation by Employee.

5.2.1. When an employee detects what appears to be a virus, the employee shall take the following steps:

5.2.1.1. Write down the name of the virus if provided by the virus detection software.

5.2.1.2. Write down any recent unusual system activities (for instance, unexpected disk access, error messages or screen displays) and, if possible, include when these activities were first noticed.

5.2.1.3. Immediately notify:

5.2.1.3.1. The office's Virus Coordinator if one has been designated; or

5.2.1.3.2. The WVBEP MIS Help Desk.

5.2.2. An office's Virus Coordinator shall take the following steps:

5.2.2.1. If the computer that may be infected is part of a network, disconnect the computer from the network.

5.2.2.2. Post a warning note on the infected computer.

5.2.2.3. Write down the name of the virus if provided by the virus detection software.

5.2.2.4. Write down any recent unusual system activities (for instance, unexpected disk access, error messages or screen displays) and, if possible, include when these activities were first noticed.

5.2.2.5. Contact the WVBEP MIS Help Desk for further assistance.

5.3. Virus Report Handling by the WVBEP MIS Division.

5.3.1. Upon receipt of a notice of a possible virus, clarify symptoms with the Virus Coordinator, verify if there is a virus, determine the source of the infection, isolate the source from the WVBEP environment, and assess the damage.

5.3.2. Verify that all potentially affected users have been notified.

5.3.3. If it is a new virus and/or the amount of damage is significant, work with the Virus Coordinator and the user(s) to isolate the virus and develop a course of action (step-by-step procedures) for restoring the network and/or computer(s) to normal.

5.3.4. Remove the virus from the affected computer, scan for viruses on any other computers that were connected to this computer, and scan any diskettes that were used in the computer(s).

Section 6. Backup and Recovery of Hard Disk.

6.1. Each employee is responsible for backing up files s/he maintains on the employee's workstation. Before backup, these files must be scanned for viruses. [NOTE: It is recommended that all files be maintained on the network server supporting the employee's workstation.]

6.2. The network administrator within The WVBEP MIS Division is responsible for the backup of all file server programs and data. As with workstation backup, the hard disk must be scanned for viruses before backup.

Section 7. Supplements and Exceptions.

7.1. Supplements to this virus protection policy may be issued by each WVBEP Division to address specific concerns or operational needs. However, any exceptions to this virus protection policy shall require prior written approval of the Director of MIS and the Commissioner of the WVBEP.

Sign: _____________________________________ Date: ____/____/____

I acknowledge that I have read the WVBEP Virus Protection Policy & Procedures on the above date.